ООО «Доктор Веб»

Компания «Доктор Веб» — российский разработчик средств информационной безопасности.

Компания «Доктор Веб» предлагает эффективные антивирусные и антиспам-решения как для государственных организаций и крупных компаний, так и для частных пользователей.

Антивирусные решения семейства Dr.Web разрабатываются с 1992 года и неизменно демонстрируют превосходные результаты детектирования вредоносных программ, соответствуют мировым стандартам безопасности

# «Руководство администратора Dr.Web Enterprise Security Suite»

Это руководство предназначено для системных администраторов, отвечающих за развёртывание, настройку и сопровождение корпоративной антивирусной инфраструктуры на базе Dr.Web. Оно охватывает всё — от первоначальной установки до тонкой настройки в крупных распределённых сетях.

**Глава 1: Введение**

**Глава 2**: **Dr.Web Enterprise Security Suite**

**2.1. О продукте** — общее описание корпоративного антивирусного решения Dr.Web: назначение, возможности, архитектура.

**2.2. Комплект поставки** — перечень компонентов, входящих в поставку (сервер, агенты, утилиты, документация).

**Глава 3:** **Лицензирование**

**3.1. Особенности лицензирования** — принципы расчёта лицензий (по числу устройств, типам ОС и т.д.).

**3.2. Распространение лицензий по межсерверным связям** — как лицензии распределяются в сетях с несколькими серверами Dr.Web.

**3.3. Автоматическое обновление лицензий** — механизм обновления лицензионных ключей без участия администратора.

**Глава 4: Начало работы**

**4.1. Создание антивирусной сети** — пошаговое формирование защищённой инфраструктуры.

**4.2. Настройка сетевых соединений** — способы подключения компонентов:

**4.2.1. Прямые соединения** — указание IP/порта вручную.

**4.2.2. Служба обнаружения Сервера Dr.Web** — автоматическое обнаружение сервера в локальной сети.

**4.2.3. Использование протокола SRV** — интеграция с DNS для автоматического поиска сервера.

**4.3. Обеспечение безопасного соединения** — настройка шифрования и защиты трафика:

**4.3.1. Шифрование и сжатие трафика** — TLS, сжатие данных.

**4.3.2. Инструменты для обеспечения безопасного соединения** — сертификаты, ключи.

**4.3.3. Подключение клиентов к Серверу Dr.Web** — процесс регистрации агентов.

**4.4. Интеграция с Active Directory** — синхронизация с AD для упрощения управления пользователями и устройствами.

**Глава 5: Компоненты антивирусной сети и их интерфейс**

**5.1. Сервер Dr.Web** — центральный компонент; управление под Windows и UNIX.

**5.2. Защита рабочих станций** — функции антивирусного агента на конечных устройствах.

**5.3. Центр управления безопасностью Dr.Web (веб-консоль)** — основной интерфейс администратора:

Администрирование, управление сетью, события, настройки, поиск, избранное, помощь.

**5.4. Компоненты Центра управления** — например, Сканер сети для автоматического обнаружения устройств.

**5.5. Схема взаимодействия компонентов** — архитектурная диаграмма и описание потоков данных.

**Глава 6: Администраторы антивирусной сети**

**6.1. Аутентификация администраторов** — поддержка различных методов:

Локальная БД, LDAP/AD, RADIUS, PAM.

**6.2. Администраторы и административные группы** — иерархия прав и делегирование полномочий.

**6.3. Управление учётными записями** — создание, редактирование, восстановление паролей, работа с группами.

**Глава 7: Комплексное управление рабочими станциями**

**7.1. Наследование конфигурации** — настройки передаются от групп к станциям.

**7.2. Группы** — системные и пользовательские; управление, размещение станций, сравнение, копирование настроек.

**7.3. Политики** — шаблоны безопасности, назначение станциям.

**7.4. Профили** — наборы параметров для быстрого развёртывания настройки.

**Глава 8: Управление рабочими станциями**

**8.1. Учётные записи станций** — подключение, удаление, объединение дублей.

**8.2. Общие настройки** — свойства, компоненты защиты, информация об оборудовании (Windows).

**8.3. Конфигурация станции** — права пользователей, расписание задач, устанавливаемые компоненты, лицензии.

**8.4. Настройка антивирусных компонентов** — параметры сканирования, обновлений и т.д.

**8.5. Антивирусная проверка** — запуск и настройка удалённых проверок.

**8.6. Статистика** — данные по угрозам, карантину, графикам, отчётам.

**8.7–8.8. Рассылка и сообщения** — массовая установка агентов и отправка уведомлений пользователям.

**Глава 9: Управление станциями в виртуальных средах**

**9.1. Подключение к Сканирующему серверу** — оптимизация защиты ВМ.

**9.2. Интеграция с VDI** — поддержка VMware, Citrix, Hyper-V и др.

**Глава 10: Настройка Сервера Dr.Web**

Обширная глава о центральном сервере:

**10.1. Управление лицензиями** — менеджер ключей, отчёты по использованию.

**10.2. Журналы** — события в реальном времени, аудит, обновления, сообщения.

**10.3. Конфигурация сервера** — настройка сети, трафика, безопасности, кеша, БД, модулей и т.д.

**10.4–10.10. Дополнительные функции** — SNMP, расписания, веб-сервер, оповещения, шаблоны сообщений.

**10.11. Управление репозиторием** — обновления, хеши угроз, содержимое.

**10.12. Контроль приложений** — белые списки, доверенные программы, тестовый режим.

**10.13. Дополнительные возможности** — резервное копирование, утилиты, статистика.

**10.14. Сеть с несколькими серверами** — кластеризация, межсерверные связи, распределённая архитектура.

**Глава 11: Обновление компонентов**

Обновление сервера, кластера, репозитория (в т.ч. в изолированных сетях).

Ограничение обновлений на станциях.

Обновление агентов в «мобильном режиме» (для ноутбуков вне сети).

**Глава 12: Настройка дополнительных компонентов**

**12.1. Прокси-сервер Dr.Web** — для маршрутизации трафика и обновлений.

**12.2. NAP Validator** — интеграция с Network Access Protection (Microsoft) для контроля соответствия политикам безопасности.

# «Приложения»

Раздел «Приложения» служит справочником для продвинутых администраторов: он содержит технические детали, CLI-параметры, конфигурационные файлы, API и решения типовых проблем — всё, что нужно для глубокой настройки и автоматизации.

**Глава 1: Введение**

**Глава 2: Приложения**

**Приложение А. Настройки для использования СУБД. Параметры драйверов СУБД**

**А1. Настройка ODBC-драйвера** — инструкция по настройке ODBC для подключения Dr.Web к базам данных.

**А2.** **Настройка драйвера БД для Oracle** — особенности конфигурации Oracle Instant Client.

**А3.** **Использование СУБД PostgreSQL** — рекомендации по установке и настройке PostgreSQL для работы с Dr.Web.

**А4.** **Использование СУБД MySQL** — параметры подключения и совместимости с MySQL.

**Приложение Б. Аутентификация администраторов**

**Б1–Б3. Аутентификация через Active Directory / LDAP / LDAP+AD** — способы интеграции с корпоративными каталогами для входа администраторов.

**Б4. Подведомственные разделы прав** — как делегировать права в иерархической структуре администраторов.

**Приложение В. Система оповещения**

**В1. Параметры системы оповещения** — настройка триггеров, условий и каналов уведомлений.

**В2. Параметры шаблонов оповещений** — формат сообщений (email, SMS, веб-уведомления).

**Приложение Г. Спецификация сетевого адреса**

**Г1. Общий формат адреса —** синтаксис указания IP, портов, доменов.

**Г2. Форматы адресов для агентов и инсталляторов** — как правильно указывать адрес сервера при развёртывании.

**Приложение Д. Управление репозиторием**

**Д1. Общие файлы конфигурации** — глобальные настройки репозитория.

**Д2. Файлы конфигурации продуктов** — параметры обновлений для конкретных компонентов (агенты, сканеры и т.д.).

**Приложение Е. Формат конфигурационных файлов**

Описание структуры ключевых конфигурационных файлов:

**Е1. Сервер Dr.Web** — основной конфиг сервера.

**Е2. Центр управления безопасностью** — настройки веб-консоли.

**Е3. download.conf** — параметры загрузки обновлений.

**Е4. Прокси-сервер Dr.Web** — конфигурация прокси.

**Е5. Загрузчик репозитория** — настройки offline-обновлений.

**Е6. share.conf** — параметры обмена данными между серверами.

**Приложение Ж. Параметры командной строки**

Список CLI-опций для ключевых компонентов:

**Ж1. Сетевой инсталлятор** — автоматическая установка агентов.

**Ж2. Агент Dr.Web для Windows** — запуск, регистрация, обновление через командную строку.

**Ж3. Сервер Dr.Web** — управление сервером из терминала.

**Ж4. Сканер Dr.Web для Windows** — параметры запуска проверок.

**Ж5. Прокси-сервер Dr.Web** — CLI-управление.

**Ж6. Инсталлятор сервера для UNIX** — установка на Linux/BSD.

**Ж7. Утилиты** — вспомогательные инструменты (резервное копирование, диагностика и др.).

**Приложение З. Переменные окружения**

Переменные, экспортируемые Сервером Dr.Web для скриптов и интеграций (например, пути, идентификаторы сессий).

**Приложение И. Регулярные выражения**

**И1–И2. PCRE в Dr.Web** — синтаксис и особенности использования регулярных выражений для фильтрации, исключений, политик.

**Приложение К. Формат файлов журнала**

Структура лог-файлов: временные метки, уровни событий, коды ошибок, формат записей.

**Приложение Л. Интеграция Web API**

Описание REST API для программного управления Dr.Web (получение статусов, запуск сканирований, управление станциями).

**Приложение М. Лицензии (сторонних компонентов)**

Юридические лицензии на open-source и коммерческие библиотеки, используемые в Dr.Web:

OpenSSL, PCRE, ICU, libssh2, Zlib, Boost, QR Code Generator и др.

(Важно для соответствия требованиям лицензирования в корпоративной среде.)

**Приложение Н. Пользовательские процедуры**

Готовые SQL-скрипты и примеры для работы с базой данных Dr.Web:

**Н1–Н10**. Управление администраторами, группами, станциями, подключениями, LDAP и др.

**Глава 3: Часто задаваемые вопросы (FAQ)**

* Практические инструкции по типичным задачам:
* Перенос сервера Dr.Web на новое «железо» (Windows / UNIX).
* Подключение агента к другому серверу.
* Оптимизация производительности и дискового пространства.
* Смена СУБД (например, с SQLite на PostgreSQL).
* Восстановление после сбоя (с резервной копией и без).
* Обновление агентов через AD/DFS.
* Управление журналами и диагностикой.
* Примеры SQL-запросов к БД сервера.

**Глава 4: Устранение неполадок**

* Диагностика удалённой установки — почему не устанавливаются агенты.
* Ошибка службы BFE (Windows) — решение проблем с брандмауэром при установке.
* Техническая поддержка — как собрать диагностические данные и обратиться в Dr.Web.

# «Руководство по установке»

Это руководство предназначено для **первоначального развёртывания** Dr.Web Enterprise: от планирования и установки до обновления и удаления. Оно охватывает все ключевые сценарии — как для небольшой школы, так и для крупного предприятия.

**Глава 1: Введение**

**Глава 2: Dr.Web Enterprise Security Suite**

**2.1. О продукте** — общее описание решения: назначение, компоненты, возможности корпоративной защиты.

**2.2. Системные требования** — минимальные и рекомендуемые требования к ОС, процессору, памяти, диску для всех компонентов (сервер, агенты, прокси и др.).

**2.3. Комплект поставки** — перечень файлов и компонентов, входящих в дистрибутив (инсталляторы, утилиты, документация).

**Глава 3: Лицензирование**

Общие принципы лицензирования Dr.Web Enterprise: как активируются ключи, как лицензируются устройства, где хранятся лицензии.

**Глава 4: Начало работы**

**4.1. Создание антивирусной сети** — пошаговое планирование развёртывания: выбор сервера, подключение клиентов, архитектура.

**4.2. Настройка сетевых соединений** — способы, как компоненты находят сервер:

**4.2.1. Прямые соединения** — указание IP/порта вручную.

**4.2.2. Служба обнаружения Сервера Dr.Web** — автоматическое обнаружение в локальной сети.

**4.2.3. Использование протокола SRV** — интеграция с DNS для автоматического поиска сервера через записи \_drweb.\_tcp.

**4.3. Обеспечение безопасного соединения** — защита трафика между компонентами:

**4.3.1. Шифрование и сжатие трафика** — использование TLS и сжатия данных.

**4.3.2. Инструменты для обеспечения безопасного соединения** — генерация сертификатов, настройка доверия.

**4.3.3. Подключение клиентов к Серверу Dr.Web** — процесс регистрации агентов с аутентификацией.

**4.4. Интеграция с Active Directory** — синхронизация с AD для автоматического размещения станций по группам и упрощения развёртывания.

**Глава 5: Установка компонентов**

**5.1. Установка Сервера Dr.Web** — центральный компонент:

**5.1.1. Для Windows** — пошаговая установка через GUI-инсталлятор.

**5.1.2. Для UNIX (Linux/BSD)** — установка через пакеты (deb/rpm) или скрипты.

**5.2. Установка Агента Dr.Web** — защита конечных устройств:

**5.2.1. Инсталляционные файлы** — типы установщиков (MSI, EXE, пакеты для Linux/macOS/Android).

**5.2.2. Локальная установка** — ручная установка на одном устройстве.

**5.2.3. Дистанционная установка** — массовое развёртывание через GPO, скрипты, Dr.Web Control Center.

**5.3. Установка Сканирующего сервера Dr.Web** — компонент для проверки почты, файловых хранилищ и виртуальных сред.

**5.4. Установка NAP Validator** — модуль для интеграции с Microsoft Network Access Protection (контроль соответствия политикам безопасности при подключении к сети).

**5.5. Установка Прокси-сервера Dr.Web** — промежуточный сервер для обновлений и связи в сегментированных сетях:

**5.5.1. Создание учётной записи** — регистрация прокси в системе.

**5.5.2–5.5.3. Способы установки** — вместе с агентом или отдельно.

**5.5.4. Подключение к Серверу Dr.Web** — настройка связи между прокси и основным сервером.

**5.6. Коды ошибок при установке** — справочник распространённых ошибок и их решений.

**Глава 6: Удаление компонентов**

**6.1. Удаление Сервера Dr.Web** — полное удаление с Windows или UNIX (включая БД и настройки).

**6.2. Удаление Агента Dr.Web** — с отдельного устройства или массово через Active Directory.

**6.3. Удаление Сканирующего сервера** — деинсталляция компонента сканирования.

**6.4. Удаление Прокси-сервера** — локальное или удалённое удаление.

**Глава 7: Обновление компонентов**

**7.1–7.2. Обновление Сервера Dr.Web** — для Windows (через инсталлятор) и UNIX (через пакетный менеджер или скрипты).

**7.3. Обновление Агентов Dr.Web** — автоматическое или ручное обновление на:

**7.3.1. Windows** — через центр управления или локально.

**7.3.2. Android** — через Google Play или корпоративный MDM.

**7.3.3. Linux/macOS** — через пакеты или скрипты.

**7.4. Обновление Прокси-сервера:**

**7.4.1. В процессе работы** — «горячее» обновление без остановки службы.

**7.4.2. Через инсталлятор** — полная переустановка с обновлением.